Cari Dudes,

Dai, tutti'nsemma:
"Debouti, le damnatos della terra..."
Grazie, Camarade.

E un grando piaccere per noi di annonsare che PAOLA ARGENTIN vai fare un' piccolo esspossato che si chiama:

ÜBER QUADRATISCHEREZIPROZITÄT (*)

Data : Lunedi 7 mai 2001
Hora : 16h15
Sallas : 6ème
Tenuta della donna : e pericoloso sporgersi.

Benvenuti a Joe le Trembleur.
Evitare vongole.

Mathieu Baillif (frappé banane)
David Cimasoni (immense canular venu de l'espace)

(*) "Signifie que les évènements ponctuels se présentent comme points isolés."

F.S.

ÜBER QUADRATISCHEREZIPROZITÄT

PAOLA “ESTIME” ARGENTIN

On veut repondre à la question suivante: quand est-ce que $m \in \mathbb{Z}$ est un carré modulo p, nombre premier impair. (C‘est-à-dire, quand est-ce que la congruence $x^2 \equiv m \pmod p$ a une solution).

Définition.
Le symbole de Legendre *est définit comme:*

$$\left(\frac{m}{p}\right) = \begin{cases} 0 & \textit{si } p \mid m \\ +1 & \textit{si } p \nmid m \textit{ et } m \textit{ est un carré} \pmod p \\ -1 & \textit{si } p \nmid m \textit{ et } m \textit{ n'est pas un carré} \pmod p \end{cases}$$

On remarque qu'il y a $\frac{p-1}{2}$ carrés dans le groupe multiplicatif du corps $\mathbb{F}_p$: $1, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$. En effet, si on considère a et $b \in \{1, \ldots, \frac{p-1}{2}\}$ et $a \neq b$, on a $a^2 \neq b^2 \pmod p$ et en outre $a^2 \equiv p - a^2 \pmod p$.

Critère d'Euler.
Soit $m \in \mathbb{Z}$ et p premier impair. Alors

$$\left(\frac{m}{p}\right) \equiv m^{\frac{p-1}{2}} \pmod p$$

Preuve:
Si $p \mid m$, c'est clair.
Si $p \nmid m$, par le Petit Théorème de Fermat on sait que $m^{p-1} \equiv 1 \pmod p$ et donc $m^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$. Supposons que $m \equiv n^2 \pmod p$, alors on a que $m^{\frac{p-1}{2}} \equiv n^{p-1} \pmod p$ où, encore par le Petit Théorème de Fermat, $n^{p-1} \equiv \pm 1 \pmod p$. Or, la congruence $m^{\frac{p-1}{2}} \equiv 1 \pmod p$ a au plus $\frac{p-1}{2}$ solutions (vu que $\mathbb{F}_p$ est un corps) et tous les carrés modulo p sont solutions. Donc $m^{\frac{p-1}{2}} \equiv 1 \pmod p \iff m$ est un carré modulo p.

D'après le Critère d'EULER, il est évident que le symbole de LEGENDRE est multiplicatif:

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$$

COROLLAIRE.
a)

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$$

b)

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \pmod p$$

Preuve:
a) Evident.
b) Soit $m \in \mathbb{Z}$, il existe un unique $r \in \mathbb{Z}$, $-\frac{p}{2} \leq r \leq \frac{p}{2}$ tel que $m \equiv r \pmod p$, on appelle r *résidu minimal* de m.
On calcule les résidus minimaux des $\frac{p-1}{2}$ éléments :$2, 4, \ldots, p-1$.
Premier cas: $p \equiv 1 \pmod 4$.
Les résidus minimaux sont: $2, 4, \ldots, \frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1$ et si on les considére en valeur absolue ils constituent l'ensemble $\{1, \ldots, \frac{p-1}{2}\}$. Le nombre des résidus minimaux négatifs est évidemment $\frac{p-1}{4}$.
Deuxième cas: $p \equiv 3 \pmod 4$.
Avec le même argument, on trouve que le nombre des résidus minimaux négatifs est évidemment $\frac{p+1}{4}$. En tout cas on remarque que $\frac{p+1}{4}$ et $\frac{p-1}{4}$ ont la même parité que $\frac{p^2-1}{8}$. On a:

$$2^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}} i = \prod_{i=1}^{\frac{p-1}{2}} 2i \equiv (-1)^{\frac{p^2-1}{8}} \prod_{i=1}^{\frac{p-1}{2}} i \pmod p$$

Donc d'après le Critère d'EULER on conclut.

LA LOI DE RÉCIROCITÉ QUADRATIQUE :
Soient p et q nombres premiers impairs distincts, on a alors que

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Preuve:
La preuve est partagée en quatre étapes.

a) Soit $m \in \mathbb{Z}$ et p premier impair qui ne divise pas m, alors les nombres $m, 2m, \ldots, \frac{p-1}{2}m$ sont non-congruents entre eux et donc leurs résidus minimaux aussi, on les appelle : $r_1, \ldots, r_\lambda, -r_1^{'}, \ldots, -r_\mu^{'}$, avec $\lambda + \mu = \frac{p-1}{2}$.
On montre que l'ensemble $\{r_1, \ldots, r_\lambda, -r_1^{'}, \ldots, -r_\mu^{'}\}$ coincide avec l'ensemble $\{1, \ldots, \frac{p-1}{2}\}$. En effet, il existe a et $b \in \{1, \ldots, \frac{p-1}{2}\}$ tels que $am \equiv r_i \pmod{p}$ et $bm \equiv r_j^{'} \pmod{p}$, si (par l'absurde) $r_i \equiv r_j^{'} \pmod{p}$ alors $(a-b)m \equiv 0 \pmod{p}$, contradiction.

b) (Avec les notations de a) où $\mu := \mu_m$)

$$\left(\frac{m}{p}\right) = (-1)^{\mu_m}$$

La preuve est semblable à celle vue pour determiner $\left(\frac{2}{p}\right)$. On a:

$$m^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}} i = \prod_{i=1}^{\frac{p-1}{2}} mi \equiv (-1)^{\mu_m} \prod_{i=1}^{\frac{p-1}{2}} i \pmod{p}$$

Donc d'après le Critère d'EULER on conclut.

c) On définit $S(p,q) = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right]$, on montre que $S(p,q)$ a la même parité de μ_q.
Soit $k \in \{1, \ldots, \frac{p-1}{2}\}$, on considère $kq = \left[\frac{kq}{p}\right] p + u_k$ $(*)$ où $u_k \in \{1, \ldots, p-1\}$.
Or, si $u_k < \frac{p}{2}$ alors u_k coincide avec un des r_i sinon, $u_k - p = -r_j^{'}$.
On dèfinit $R = \sum_i^\lambda r_i$ et $R^{'} = \sum_j^{\mu_q} r_j^{'}$
Or,

$$\frac{p^2-1}{8} = R + R^{'} = \sum_{k|u_k<\frac{p}{2}} u_k + p\mu_q - \sum_{k|u_k>\frac{p}{2}} u_k$$

On réduit modulo 2:

$$\frac{p^2-1}{8} \equiv \sum_{k=1}^{\frac{p-1}{2}} u_k + \mu_q \pmod{2} \tag{1}$$

Mais d'après $(*)$, en sommant sur k, on obtient

$$q\frac{p^2-1}{8} = pS(p,q) + \sum_{k=1}^{\frac{p-1}{2}} u_k.$$

On réduit modulo 2:

$$\frac{p^2-1}{8} \equiv S(p,q) + \sum_{k=1}^{\frac{p-1}{2}} u_k \pmod{2} \tag{2}$$

En remplaçant (2) dans (1), on conclut que $S(p,q) \equiv \mu_q \pmod 2$.

d) On montre que $S(p,q) = \frac{p-1}{2}\frac{q-1}{2}$.
On considère le rectangle de côtés $[1,\dots,\frac{p-1}{2}] \times [1,\dots,\frac{q-1}{2}]$. Le nombre de points ayant coordonées entières est $\frac{p-1}{2}\frac{q-1}{2}$.
On va compter différemment ces points: on considère la droite $y = \frac{q}{p}x$ et on compte les points à coordonnées entières qui sont au-dessous et au-dessus de telle droite. Ils sont respectivement:
$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right] = S(p,q) \equiv \mu_q \pmod p$ et $\sum_{l=1}^{\frac{q-1}{2}} \left[\frac{lp}{q}\right] = S(q,p) \equiv \mu_p \pmod q$.
Donc

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu_p+\mu_q} = (-1)^{S(p,q)+S(q,p)} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Exemple :
On veut determiner si 219 est un carré modulo 383.
On étudie le symbole de Legendre $\left(\frac{219}{383}\right)$ en utilisant la multiplicativité, la loi de réciprocité, la valeur de $\left(\frac{-1}{p}\right)$ et $\left(\frac{2}{p}\right)$.
Vu que 219=3*73, la multiplicativité implique:

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right)\left(\frac{73}{383}\right).$$

En utilisant réciprocité, on a:

$$\left(\frac{3}{383}\right) = \left(\frac{383}{3}\right)(-1)^{\frac{(383-1)(3-1)}{4}} = -\left(\frac{-1}{3}\right) = -(-1)^{\frac{3-1}{2}} = 1$$

et

$$\left(\frac{73}{383}\right) = \left(\frac{383}{73}\right)(-1)^{\frac{(383-1)(73-1)}{4}} = \left(\frac{18}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{9}{73}\right) = (-1)^{\frac{(73)^2-1}{8}} = 1.$$

Alors $\left(\frac{219}{383}\right) = 1$, donc 219 est un carré modulo 383.